★MITQ P85;T01 2000-437266/38 ★JP 2000155524-A

Electronic seal approval system for use in enterprise, confirms signature of person and text using disclosure key in approved text data, approving person's signature and text and displays approval

MITSUBISHI ELECTRIC CORP 1998.11.19 1998JP-328955
W01 (2000.06.06) G09C 1/00, G06F 13/00, 15/00, H04L 9/32

Novelty: Correctness of approving person (3) is confirmed based on input data decoded using a disclosure key, authentication document output by server (5) and sealing time data, upon demand from client. After authentication, combined text, person's signature, authentication document and data (7) approved by client (4) are output to client (9) which confirms correctness of person (3) and text using received data.

Detailed Description: An authentication server (1) outputs authentication document of signature and disclosure key of the document is written to IC card (2) and output to approving person (3). The person (3) inputs data (6) to client (4) which processes the input using the authentication document and key and generates approved data (7). The correctness of rating, sealing time is confirmed using disclosure key extracted from notary signature which is generated using private key by client (4) and approval person's command, approved data. The text and the approved comment are then displayed.

Use: In enterprise to process proof mark.

Advantage: Certification can be trusted reliably as server outputs signature as a notary third person signature and hence is neutral.

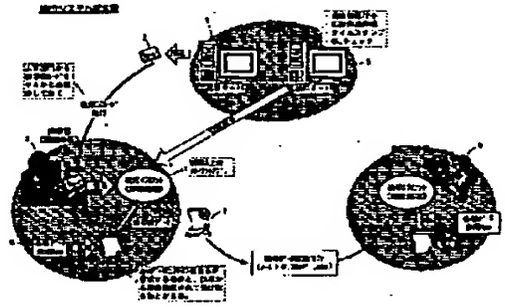
Description of Drawing(s): The figure shows the conceptual diagram of the approval system.

Authentication server 1
IC card 2
Person 3
Client 4,9
Server 5
Data 6,7
(8pp Dwg.No.1/3)

N2000-327169

A2

T01-H07C5S; T01-J12C; W01-A05B



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－155524
（P2000－155524A）
(43)公開日　平成12年６月６日(2000.6.6)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｂ	５Ｂ０８５
			６４０Ｚ	５Ｂ０８９
	６６０		６６０Ｅ	５Ｊ１０４
Ｇ０６Ｆ　13/00	３５４	Ｇ０６Ｆ　13/00	３５４Ｚ	
15/00	３３０	15/00	３３０Ａ	

審査請求　未請求　請求項の数３　ＯＬ　（全　８　頁）　最終頁に続く

(21)出願番号　特願平10－328955

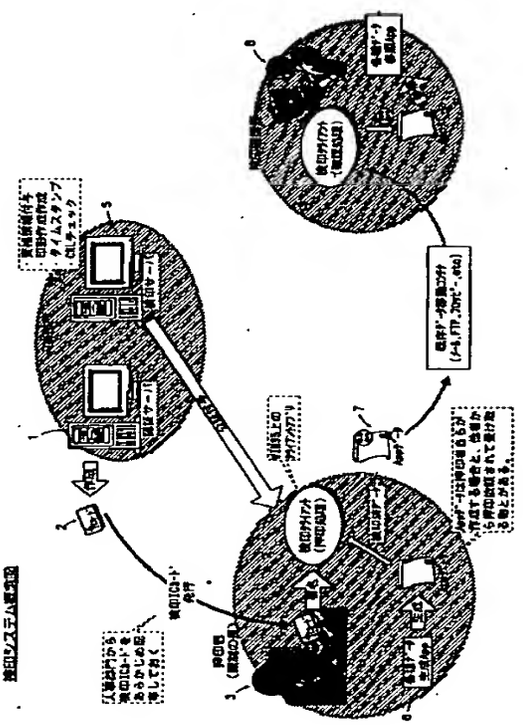
(22)出願日　平成10年11月19日(1998.11.19)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　桧山　秀郎
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100102439
弁理士　宮田　金雄　（外２名）

Ｆターム(参考)　5B085 AE23 AE29 BG07
5B089 GA01 GA12 GA21 GB03 GB09
JA16 JA40 JB01 JB03 KA00
KB11 KC58 KH30
5J104 AA09 AA11 LA03 LA06 MA02
NA35 PA07

(54)【発明の名称】　電子検印システム

(57)【要約】
【課題】　検印者自身による署名機能の他に、第三者による検印日時の証明、検印者の正当性の証明、検印者の職務上の資格証明及び印影画像情報の付与を同時に行う電子検印システムを提供する。
【解決手段】　認証サーバ１は認証書を発行し、認証書と対応するプライベート鍵はＩＣカード２に入れて検印者３に配布しておく。検印者３は検印が必要な電子的な原データ６を検印クライアント４の入力データとして入力する。検印クライアントはＩＣカード内の認証書とプライベート鍵を利用し、同時に検印サーバ５に対して公証付与を依頼して得られた公証結果を原データ６と組み合わせて検印済データ７を生成する。この検印済データ７はＨＴＴＰ、ＦＴＰ、フロッピー（登録商標）などのメディアを通じて検印確認者８に送信される。検印確認者８が検印検証ソフトウェア９の入力データとして検印済データ７を入力することにより検印の正当性が確認できる。



【特許請求の範囲】
【請求項１】　認証サーバと、押印処理検印クライアントと、検印サーバと、確認処理用（以下、検証用ともいう）検印クライアントを備え、上記認証サーバは、検印者のデジタル証明書（以下、認証書ともいう）と公開鍵方式のプライベート鍵を発行して検印者にＩＣカード等により配布し、上記押印処理検印クライアントは、上記検印者が上記プライベート鍵を用いて署名を行う検印者署名手段と、上記検印者による原文用検印者署名と公証依頼用検印者署名による出力データと検印者の認証書を送信して公証の付与を依頼し、上記検印サーバは、資格情報と時計と印影画像を有し、上記押印処理検印クライアントからの公証付与の依頼を受信すると、受信した出力データを上記検印者の公開鍵を用いて復号したデータと受信した認証書とに基づいて検印者の正当性を確認し、時計情報から押印日時を生成するとともに、検印者の資格情報と印影画像を検索してこの押印日時と検印者の資格と印影画像と原文用検印者署名とに基づいて検印サーバ自身の公開鍵方式のプライベート鍵を用いて公証人署名を行い、上記押印日時と検印者の資格と印影画像と公証人署名と公証人の認証書を公証として上記押印処理検印クライアントに送付し、上記押印処理検印クライアントは、上記公証を上記検印サーバから受信すると、上記押印日時と検印者の資格と印影画像と公証人署名と公証人の認証書に原文と検印者コメントと原文用検印者署名と検印者の認証書とを合わせて検印済みデータとして生成し、上記確認処理用検印クライアントに送信し、上記確認処理用検印クライアントは、上記押印処理検印クライアントからの検印済みデータを受信すると、該検印済みデータ中の原文と検印者コメントと原文用検印者署名と検印者の認証書と該検印者の認証書から取り出した公開鍵を用いて原文と検印者コメントの非改竄性を確認すると同時に検印者の正当性を確認し、次に公証人署名と押印日時と検印者の資格と印影画像データと原文用検印者署名と公証人の認証書と該公証人の認証書から取り出した公開鍵を用いて検印者の資格と押印日時の正当性と公証人の正当性を確認し、上記検印済みデータから原文と検印者コメントを取り出し、該原文及び検印者コメントを表示することを特徴とする電子検印システム。
【請求項２】　押印処理検印クライアントは、検印者による押印の際、原文に検印者自身のコメントを付加した後、電子署名を行うことを特徴とする請求項１に記載の電子検印システム。
【請求項３】　押印処理検印クライアントと検印サーバ間の通信、及び押印処理検印クライアントと確認処理用検印クライアント間の通信として、ＨＴＴＰプロトコルなどの通信プロトコルによる通信手段、ＦＴＰプロトコルによるＦＴＰ通信手段、電子メールのプロトコルによる電子メール通信手段、フロッピーディスク等の可搬性データストレージメディアのいずれをも接続することを特徴とする請求項１に記載の電子検印システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、企業内業務で通常使用されている検印の電子化や行政分野で利用されている証明印の電子化を行う電子検印システムに関するものである。
【０００２】
【従来の技術】従来の電子署名方式は例えば特開平７－２８７５１５号公報に示されている。ここでは、認証交換と電子署名の方法について各種の方法が説明されているが、これらはシュノールの認証交換方法をベース（従来例）としてさらに改良を加えたものであり、内容は複雑になっているが本質的な考え方はシュノールの認証交換方法と同じである。
【０００３】ここでは、説明を簡単にするために、従来例としてシュノールの認証交換方法について説明する。図３はシュノールの認証交換方法の概略図である。図において、まず、素数ｐ、ｑを用意する。証明者Ａは検証者Ｂに自身を証明するために、１とｑとの間のランダムな数ｒを生成し、１とｐとの間のランダムな数ｇを生成する。次に、ｇをｒで累乗し、これをｐで割った残りｘ（$x=g^r \bmod p$）を求める。そして、このｘを検証者Ｂに送信する。検証者Ｂは証明者Ａからｘを受信すると、１とｑとの間でランダムな数ｅを生成して証明者Ａへ送信する。証明者Ａは、検証者Ｂからランダムな数ｅを受信すると、このｅと自分の秘密鍵の１つであるｓと掛け、これに上記で用いたランダムな数ｒを加えてｑで割った残りｙ（$y=(r+es) \bmod p$）を求める。そしてこのｙを検証者Ｂへ送信する。
【０００４】検証者Ｂは証明者Ａからこのｙを受信すると、ｇをｙで累乗し、これに証明者Ａの公開鍵であるｖ（$v=v^{-s} \bmod p$）をｅで累乗して掛けた後、ｐで割った残り（$g^r v^s \bmod p$）を求める。このようにして求めた残りが証明者Ａから受信したｘ（$x=g^r \bmod p$）と同じであるか否かを調べて証明者Ａの正当性を認証する。
【０００５】また、検証者Ａは１とｑとの間でランダムな数ｒを生成してｇをｒで累乗し、これをｐで割った残りｘ（$x=g^r \bmod p$）を求める。そして、ハッシュ関数を用いてｘと文書ｍをハッシュ（縮約）し、ｅ（$e=h(g^r \bmod p, m)$）を求める。さらに、文書ｍに対する署名者Ａの電子署名を検証できるよう自分の秘密鍵であるｓとｅを掛け、これに用いられたランダムな数ｒを加えてｑで割った残りｙ（$y=(r+es) \bmod q$）を求める。このようにして求めた（ｅ、ｙ）が、文書ｍに対する署名者Ａの電子署名となる。
【０００６】文書ｍに対する署名者Ａの電子署名（ｅ、ｙ）の検証では、ｇをｙで累乗し、これに署名者Ａの公

開鍵であるｖ（ｖ＝v^{-s} ｍｏｄ ｐ）をｅで累乗して掛けた後、ｐで割った残り（g^r v^s ｍｏｄ ｐ）を求める。そして、これと文書ｍをハッシュする。このようにハッシュした値 ｈ（g^r v^s ｍｏｄ ｐ、ｍ）が受信したｅと同じであるか否かを調べることにより、署名者Ａの電子署名（ｅ、ｙ）の正当性を検証する。

【０００７】

【発明が解決しようとする課題】このように、従来の電子署名方法では、確かに検印者の資格の証明と電子署名の正当性の検証ができるが、検印時の検印日時の証明や検印者の正当性の証明や検印者の資格の証明を中立で信頼できる第三者によって保証する手段がなく、悪意の検印者がいた場合の対抗手段がないという問題点があった。

【０００８】また、従来の電子署名では検印画像データを扱っておらず、従来の電子署名に実社会で使われている検印画像データを単純に電子的に付加しただけでは電子署名本来の機能に馴染まなかった。従って、従来の電子署名と実社会における検印業務の機能との対応がとりにくく、そのために広く普及しづらいという問題点があった。

【０００９】この発明は上記のような問題点を解消するために為されたものであり、実社会で用いられている検印業務を電子的に実現するために、検印者自身による署名機能の他に、第三者による検印日時の証明、検印者の正当性の証明、検印者の職務上の資格証明および印影画像情報の付与を同時に行うことを目的とする。

【００１０】

【課題を解決するための手段】この発明に係る電子検印システムは、認証サーバと、押印処理検印クライアントと、検印サーバと、確認処理用（以下、検証用ともいう）検印クライアントを備え、上記認証サーバは、検印者のデジタル証明書（以下、認証書ともいう）と公開鍵方式のプライベート鍵を発行して検印者にＩＣカード等により配布し、上記押印処理検印クライアントは、上記検印者が上記プライベート鍵を用いて署名を行う検印者署名手段と、上記検印者による原文用検印者署名と公証依頼用検印者署名による出力データと検印者の認証書を送信して公証の付与を依頼し、上記検印サーバは、資格情報と時計と印影画像を有し、上記押印処理検印クライアントからの公証付与の依頼を受信すると、受信した出力データを上記検印者の公開鍵を用いて復号したデータと受信した認証書とに基づいて検印者の正当性を確認し、時計情報から押印日時を生成するとともに、検印者の資格情報と印影画像を検索してこの押印日時と検印者の資格と印影画像と原文用検印者署名とに基づいて検印サーバ自身の公開鍵方式のプライベート鍵を用いて公証人署名を行い、上記押印日時と検印者の資格と印影画像と公証人署名と公証人の認証書を公証として上記押印処理検印クライアントに送付し、上記押印処理検印クライアントは、上記公証を上記検印サーバから受信すると、上記押印日時と検印者の資格と印影画像と公証人署名と公証人の認証書に原文と検印者コメントと原文用検印者署名と検印者の認証書とを合わせて検印済みデータとして生成し、上記確認処理用検印クライアントに送信し、上記確認処理用検印クライアントは、上記押印処理検印クライアントからの検印済みデータを受信すると、該検印済みデータ中の原文と検印者コメントと原文用検印者署名と検印者の認証書と該検印者の認証書から取り出した公開鍵を用いて原文と検印者コメントの非改竄性を確認すると同時に検印者の正当性を確認し、次に公証人署名と押印日時と検印者の資格と印影画像データと原文用検印者署名と公証人の認証書と該公証人の認証書から取り出した公開鍵を用いて検印者の資格と押印日時の正当性と公証人の正当性を確認し、上記検印済みデータから原文と検印者コメントを取り出し、該原文及び検印者コメントを表示するものである。

【００１１】また、この発明に係る電子検印システムは、押印処理検印クライアントは、検印者による押印の際、原文に検印者自身のコメントを付加した後、電子署名を行うものである。

【００１２】また、この発明に係る電子検印システムは、押印処理検印クライアントと検印サーバ間の通信、及び押印処理検印クライアントと確認処理用検印クライアント間の通信として、ＨＴＴＰプロトコルなどの通信プロトコルによる通信手段、ＦＴＰプロトコルによるＦＴＰ通信手段、電子メールのプロトコルによる電子メール通信手段、フロッピーディスク等の可搬性データストレージメディアのいずれをも接続するものである。

【００１３】

【発明の実施の形態】実施の形態１．図１はこの発明に係る検印システムの一実施の形態を示す概念図であり、この検印システムを一企業内に適用した場合の運用の全体の流れを示している。図において、１はデジタル証明書（以下、認証書ともいう）を発行する認証サーバ、２は発行されたデジタル証明書を格納するＩＣカード、３は検印処理を行う検印者、４は検印者３が検印処理を行う際の検印者側のソフトウェアを示す押印処理用検印クライアント、５は検印クライアント４からの依頼に基づき中立の第三者として時刻情報、検印者資格、印影画像データを付与する検印サーバ、６は検印を受ける原データ、７は検印処理後の検印済データ、８は検印済データ７を検証する検証者（以下、検印確認者ともいう）、９は検証者８が検証を行う際の検証者側のソフトウェアを示す検印クライアントである。

【００１４】次に、図１に示した運用の流れを説明する。検印者は、予め検印者の正当性を保証するための認証書と、この認証書と対になったプライベート鍵（公開鍵方式のプライベート鍵）の発行をシステムの運用部門

から受けておく。この場合、認証書の発行は通常は認証サーバ1が行い、認証書と対応するプライベート鍵はICカード2等の媒体に入れて検印者に配布される。

【0015】検印者（通常職制の長であり押印者を指す）3は検印が必要な電子的な原データ6（この原データは各種のデータ生成用アプリケーションによって生成される）を押印処理用検印クライアント4の入力データとして入力し、検印済データ7を出力する。このとき、検印クライアントはICカード2内の認証書とプライベート鍵を利用し、同時に検印サーバ5に対して公証付与を依頼して得られた公証結果を原データと組み合わせて検印済データ7を生成している。検印確認者8は検印クライアント4からの検印済データ7を入力し、検印検証ソフトウェアである検印クライアント9により検印の正当性を確認することができる。

【0016】図2は図1における検印処理の詳細な処理の流れを示した説明図であり、特に、ファイル類の流れについて説明している。図中、図1と同符号は同一又は相当部分を示す。101は検印クライアント4による一次処理、102は押印処理用検印クライアント4から検印サーバ5への依頼データ、103は検印サーバ5による処理、104は検印サーバ5から押印処理用検印クライアント4へのレスポンス、105は押印処理用検印クライアント4による2次処理である。なお、検印サーバ5は資格管理DB（データベース）、日付情報及び検印画像データを管理しているものとする。

【0017】次に、動作を図2を用いて説明する。押印処理用検印クライアント4による1次処理101において、まず、原文に対して検印者によるコメントを付与し、次に原文とコメントを合わせたデータ全体に対して検印者による原文用電子署名を作成する。さらに、この原文用電子署名と検印者自身の認証書を合わせたデータに対して、公証依頼用電子署名を生成する。なお、ここでいう電子署名とは署名対象のデータをハッシュ関数（一方向性関数）の入力値とし、ハッシュ関数を通して得られた出力値を検印者の持つ公開鍵方式のプライベート鍵で暗号化したデータである。これにより、他人によるデータの改竄などを防止できる。なお、ハッシュ関数を用いるのは、暗号化の高速化を図る為である。

【0018】次に、検印クライアント4から検印サーバ5へ公証付与の依頼を行う。この場合、押印処理用検印クライアント4は一次処理101で作成した原文用検印者署名と検印者自身の正当性を示す認証書と公証依頼用検印者署名を合わせて依頼データ102を作成し、検印サーバ5へ送付する。

【0019】検印サーバ5はこの依頼データ102を押印処理用検印クライアント4から受信すると、依頼データ102中の原文用検印者署名と検印者自身の正当性を示す認証書から原文用検印者署名の非改竄性と公証依頼者（検印者）の正当性を調べる。この場合、検印者の公開鍵を用いて公証依頼用検印者署名を復号したデータを、認証書と原文用検印者署名をハッシュ関数を通して得られた出力値と照合する。照合の結果一致しなければ、検印サーバ5はその旨（エラー）を検印クライアントに通知する。照合の結果、一致して正当性が証明されると、検印サーバ5は原文用検印者署名を取り出す。

【0020】次に、検印サーバ5は自身が管理している資格管理DB（データベース）から検印者の資格情報を取り出し、これと公証依頼時の日付から印影画像データを生成する。次に、検印サーバ5は原文用検印者署名と資格情報と日付情報と検印画像データを合わせたものに対してハッシュ関数を通して、得られたデータに公開鍵方式の公証人のプライベート鍵で暗号化し、公証人署名を生成する。これにより、他人によるデータの改竄などを防止できる。

【0021】次に、検印サーバ5はレスポンスとして押印処理用検印クライアント4へ公証付与を行う。この場合、検印サーバ5は上記処理103で生成した公証人署名と資格情報と日時情報と印影画像データと公証人の認証書をまとめて公証付与済データ104を作成し押印処理用検印クライアント4に送付する。

【0022】押印処理用検印クライアント4はこの公証付与済データ104を検印サーバ5から受信すると、押印処理用検印クライアント4側での2次処理105において、公証付与済データとして受け取った公証人署名と資格情報と日付情報と印影画像データに原文用検印者署名と検印者コメントと原文を合わせ、さらに公証人の認証書と検印者の認証書を加えたものを1つのファイルとして生成する。このファイルが検印付与済の原文データとなる（以下、検印済みデータともいう）。

【0023】次に、押印処理用検印クライアント4は検印付与済みの原文データを既存のデータ移動コンテナ即ちファイル転送や電子メール、フロッピーなどの通信媒体によって確認処理用検印クライアント（検証用検印クライアントともいう）9に送付する。

【0024】確認処理用検印クライアント9は、押印処理用検印クライアント4からの検印済みデータを受信すると、この検印済みデータ中の原文と検印者コメントを合わせたものをハッシュ関数にかけて得られたデータと原文用検印者署名を検印者の公開鍵を用いて復号したデータとを照合する。照合の結果一致しなければ、その旨を画面にエラー表示し、一致すれば原文と検印者コメントの非改竄性が証明できたことになる。

【0025】確認処理用検印クライアント9は、更に検印者の認証書の正当性も検証することにより検印者の正当性を確認する。次に、確認処理用検印クライアント9は、原文用検印者署名と資格情報と日時情報と印影画像データを合わせたものにハッシュ関数をかけて得られたデータと公証人署名を公証人の公開鍵を用いて復号したデータとを照合する。照合の結果一致しなければ、その

旨を画面にエラー表示し、一致すれば原文と検印者コメントの非改竄性を確認したと同時に検印日時と検印者の資格が正しいことを公証人からお墨つきを頂いたことを示すので、検証用検印クライアント９は上記検印済みデータから原文と検印者コメントと印影画像データを取り出し、これらを表示する。

【００２６】この実施の形態によれば、検印時の検印日時の証明や検印者の正当性の証明や検印者の資格の証明を中立で信頼できる第三者によって保証することができる。

【００２７】また、この実施の形態によれば、検印者による押印の際、押印対象である原文に検印者自身のコメントを付加した後、電子署名を行うことにより、従来紙に対して押印を行う際に検印者の朱書きコメントを書き込むことに相当する機能を実現することができる。

【００２８】また、この実施の形態によれば、検印者用の端末と、検印サーバは双方ともＨＴＴＰプロトコルなどの通信プロトコルにより通信を行うための通信手段と、ＦＴＰプロトコルにより通信を行うためのＦＴＰ通信手段と、電子メールプロトコルにより通信を行うための電子メール通信手段と、フロッピーディスク等の可搬性データストレージとを備えたので、検印者と検印サーバとの通信はＨＴＴＰプロトコルなどの通信プロトコル、ＦＴＰプロトコル、電子メールプロトコル、フロッピーディスク等の可搬性データストレージメディアのいずれでも可能である。

【００２９】

【発明の効果】以上、この発明によれば、検印サーバが検印者の資格や日時や印影画像データに対して第三者である公証人としての署名をするので、検印時の検印日時の証明や検印者の正当性の証明や検印者の資格の証明を中立で信頼できる第三者によって保証することができるという効果を奏する。

【００３０】また、この発明によれば、検印者による押印の際、押印対象である原文に検印者自身のコメントを付加した後、電子署名を行うので、従来の紙に対して押印を行う際に検印者の朱書きコメントを書き込むことに相当する機能を実現することができるという効果を奏する。

【００３１】また、この発明によれば、押印処理検印クライアントと検印サーバ間の通信、及び押印処理用検印クライアントと確認処理用検印クライアント間の通信として、ＨＴＴＰプロトコルなどの通信プロトコルによる通信手段、ＦＴＰプロトコルによる通信手段、電子メールのプロトコルによる通信手段、フロッピーディスク等の可搬性データストレージメディアのいずれをも接続するので、ＨＴＴＰプロトコルなどの通信プロトコルによる通信、ＦＴＰプロトコルによる通信、電子メールプロトコルによる通信、フロッピーディスク等の可搬性データストレージメディアによる通信のいずれも可能であるという効果を奏する。

【図面の簡単な説明】

【図１】　この発明に係る検印システムの一実施の形態を示す概念図である。

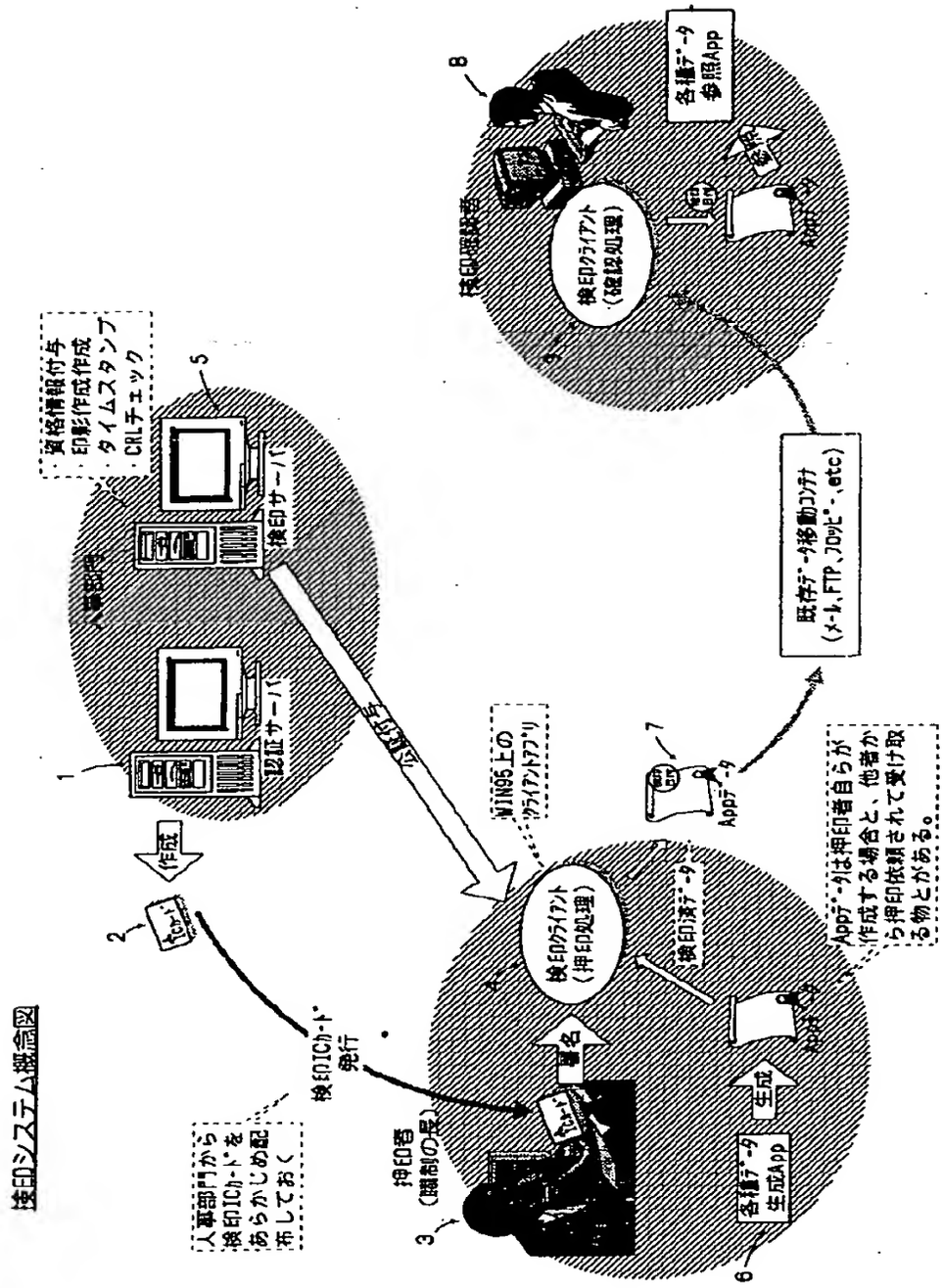
【図２】　実施の形態１における検印処理を行う際の詳細な処理の流れを示した説明図である。

【図３】 従来の電子署名を示すシュノールの認証交換方法の概略図である。

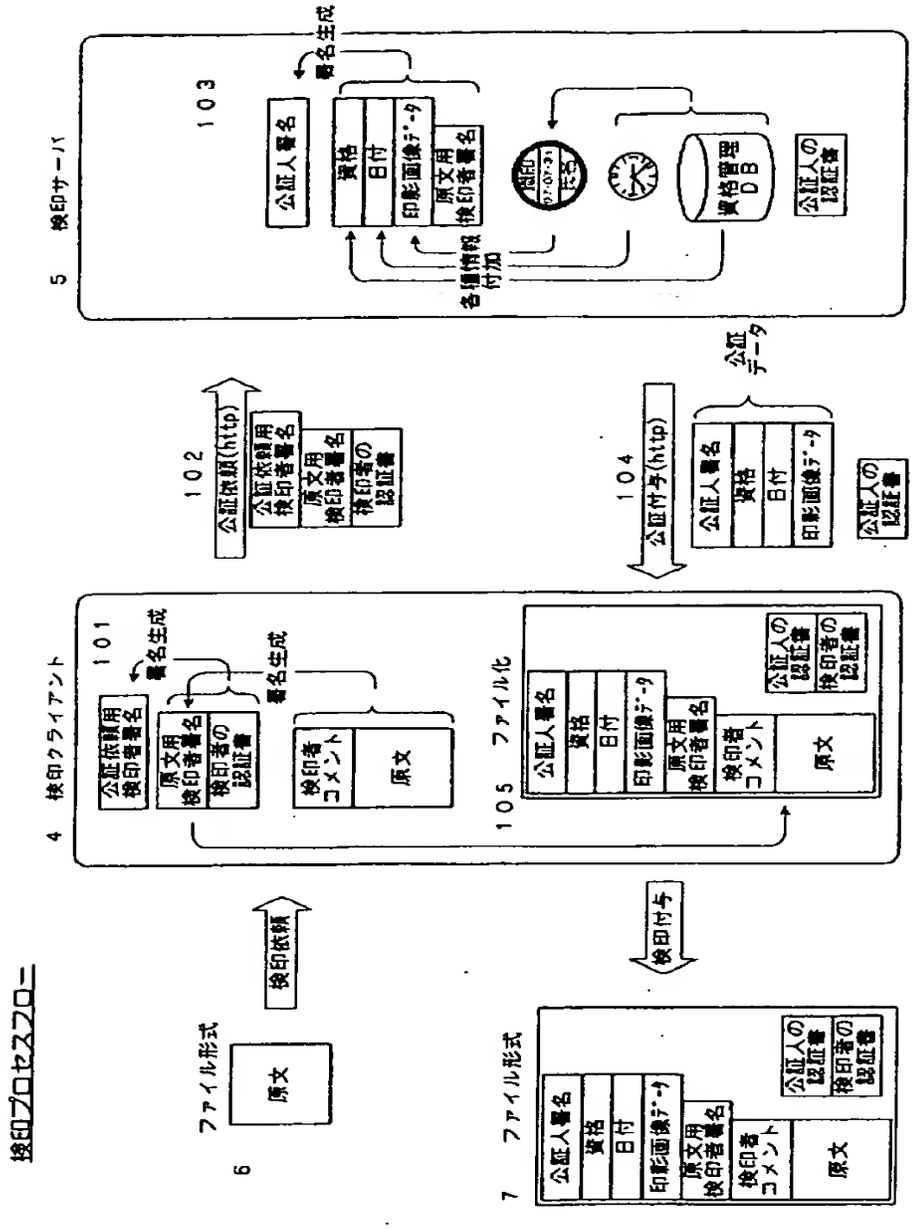
【符号の説明】

１　認証サーバ
２　ＩＣカード
３　押印者
４　検印クライアント（押印処理）
５　検印サーバ
６　原文データ
７　検印済データ
８　検印確認者
９　検印クライアント（確認処理）

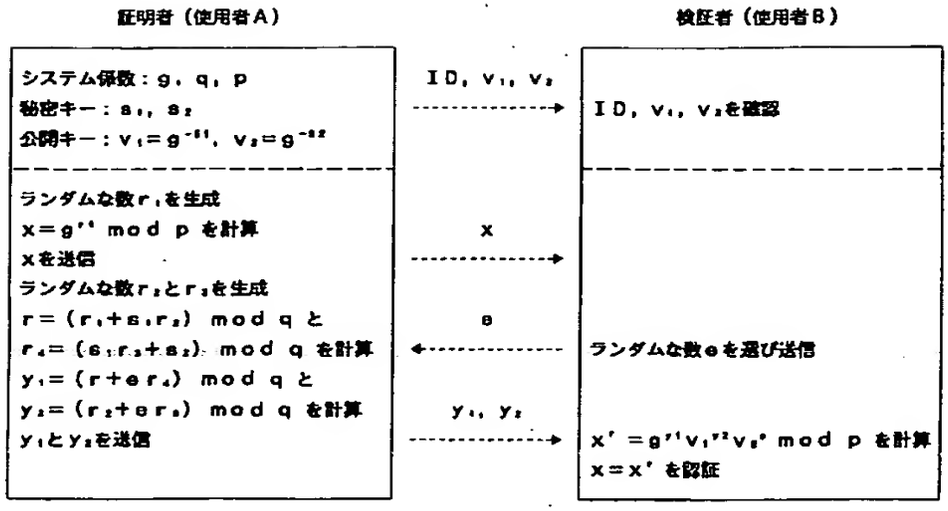
【図1】


捺印システム概念図
人事部門
資格情報付与
印影作成作成
タイムスタンプ
CRLチェック
捺印サーバ
認証サーバ
作成
捺印ICカード発行
人事部門から捺印ICカードをあらかじめ配布しておく
捺印者（職制の長）
暗号
捺印クライアント（押印処理）
捺印済データ
生成
各種データ生成App
Appデータ
Appデータは押印者自らが作成する場合と、他者から押印依頼されて受け取る物とがある。
WIN95上の捺印クライアントアプリ
Appデータ
既存データ移動コンテナ（メール、FTP、JDyビ゛、etc）
捺印確認者
捺印クライアント（確認処理）
各種データ参照App
Appデータ
1
2
3
4
5
6
7
8
9

【図2】


検印プロセスフロー
ファイル形式
原文
6
検印依頼
4 検印クライアント
101
公証依頼用検印者署名
原文用検印者署名
検印者の認証書
署名生成
検印者コメント
原文
102
公証依頼(http)
公証依頼用検印者署名
原文用検印者署名
検印者の認証書
5 検印サーバ
103
公証人署名
資格
日付
印影画像データ
原文用検印者署名
署名生成
各種情報付加
印影データ
資格管理DB
公証人の認証書
104
公証付与(http)
公証データ
公証人署名
資格
日付
印影画像データ
公証人の認証書
検印付与
7 ファイル形式
105 ファイル化
公証人署名
資格
日付
印影画像データ
原文用検印者署名
検印者コメント
原文
公証人の認証書
検印者の認証書

【図3】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI		テーマコード（参考）
H04L 9/32		H04L 9/00	673D	
			675B	
			675D	